FOREWORD

The Risk Management Plan (RMP) is developed to provide the Program Manager for the Integrated Terminal Weather System (ITWS) with a structured approach to risk identification and management. The ITWS program has already initiated an extensive risk management effort through its demonstration/validation program. Continued focus on identification and risk mitigation of cost, schedule and technical risks will help the program reach its objectives. This RMP was developed in accordance with FAA Order 1810.1F, Major Systems Acquisitions.

Kenneth Klasinski, Manager
Aviation Weather Development Program

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to define a structured approach to risk identification and management for the Integrated Terminal Weather System (ITWS) program. The risk management process described herein will be implemented and maintained by the ITWS Program Manager (PM) throughout the ITWS program. This plan is applicable to both government and ITWS prime contractor risk management activities leading to the successful deployment and life cycle support of the initial operational capability (IOC).

1.2 Background

The ITWS is a development program initiated by the Federal Aviation Administration (FAA) to produce a fully-automated, integrated terminal weather information system to improve the safety, efficiency and capacity of terminal area aviation operations. The ITWS will acquire data from FAA and National Weather Service sensors as well as from aircraft in flight in the terminal area. The ITWS will produce products to Air Traffic personnel that are immediately usable without further meteorological interpretation. These products include current terminal area weather and short-term (0-30 minute) predictions of significant weather phenomena.

1.3 Applicable Documents

1.3.1 FAA Documents

a) FAA-ORD-1810.1F, Major Systems Acquisition, Mar 1993
b) ITWS Operational Requirements Document (ORD), Oct 1994
c) ITWS Cost benefit Analysis, Oct 1994
d) ITWS Test and Evaluation Master Plan (TEMP), Oct 1994
e) ITWS Acquisition Plan, Oct 1994
f) ITWS Maintenance Requirements Document, Oct 1994
g) ITWS Program Implementation Plan, Oct 1994

1.3.2 Contractor Documents (When approved by the FAA)

a) CDRL-XXXXProgram Management Plan
b) CDRL-XXXX Program Status Report
c) CDRL-XXXX Program Risk Management Plan

1.3.3 Other Documents

a) Final Report for the Air Traffic Control (ATC) Operational Evaluation of the Prototype Integrated Terminal Weather System (ITWS) at Dallas/Fort Worth (DFW) and Orlando International (MCO) airports, May-September 1993

b) Final Report for the Air Traffic Control (ATC) Operational Evaluation of the Prototype Integrated Terminal Weather System (ITWS) at Memphis (MEM) and Orlando International (MCO) airports, May-September 1994

1.4 Definition of Terms

Risk management - Risk management is a methodology for systematically identifying the elements or events that could potentially cause undesired effects (cost overruns, schedule delays, performance degradation, etc), and executing appropriate measures to reduce or eliminate both the impact and the occurrence of such elements or events. It is an integral part of program management rather than an independent and isolated function. As with all program management functions, risk management must be integrated into the day-to-day activities of all program personnel. In so doing risk management becomes a natural part of all program processes rather than an artificially and externally imposed system. Just as quality must be designed in rather than inspected in, risk must be designed out rather than analyzed out.

Low risk - Low risk is a condition where a risk is identified and its occurrence would have a minor effect or consequence on program objectives. No special program emphasis is required other than normal monitoring and control by the person allocated the responsibility for that relevant task.

Moderate risk - Moderate risk is a condition where a risk is identified and its occurrence would affect program objectives. This level of risk should be carefully monitored and discussed at program reviews. A risk mitigation plan should be developed.

High risk - High risk is a condition where the consequence would have a significant impact on the program. The PM will ensure that control and monitoring of each high risk element will occur. A risk mitigation plan is mandatory and the highest level of program priority will be placed on reducing the risk.

Risk element - A risk element is a facet of the development, management, or maintenance of the system or program which is identified as having potential risk.

1.5 Risk Planning

1.5.1 Controlling Documents

1.5.1.1 ITWS Risk Management Plan (RMP)

The ITWS RMP is the controlling document for the management of all risks associated with the ITWS program. It will be updated periodically to reflect changes in risk mitigation strategies which are the natural outcome of the continual risk identification and mitigation process.

1.5.1.2 Contractor Program Risk Management Plan (PRMP)

The contractor's PRMP will be the primary document for the mitigation of risks identified in the contractor's area of responsibility. The content of the contractor's PRMP is outlined in accordance with the ITWS program Data Item Description (DID). The DID content is summarized below:

a) Introduction: 1) Purpose; 2) Applicable Documents/Definitions; 3) Management Responsibilities and Organizational Structure; and 4) Scheduled Milestones/Reviews.

b) Procedures for Risk Management: 1) Identification of risk elements; 2) Assessment of the risk factors identified; 3) Assignment of appropriate resources to reduce risk factors; 4) Identification and analysis of the alternative actions available; 5) Identification of the most promising alternatives; 6) Implementation plan; 7) Risk-reducing action feedback procedure; and 9) Risk- reduction schedule.

c) Risk Assessment Analysis, and Reduction: A risk mitigation plan and/or strategy will be developed for identified risk elements.

1.5.2 Roles and Responsibilities

The PM will have ultimate responsibility for managing, directing, and authorizing ITWS risk management activities. This responsibility will include establishing the roles and responsibilities for the program, delegating authority for the risk management plan and process, participating in reviews of

program risks, establishing program policies for handling and accepting risk, approving and directing risk reduction strategies, and ensuring that appropriate priority is placed on the conduct of these activities.

The PM will identify a resource to act as the *risk coordinator*. The coordinator will facilitate risk management process execution including, as appropriate: assisting program team resources in risk identification and assessment, maintaining risk data bases, monitoring risk reduction progress, and generating reports at the discretion of the PM. The PM will have ultimate authority concerning matters of risk level assessment, and mitigation strategy. The PM will determine and/or approve the level of resource, and the schedule to be applied to mitigation strategies for risks identified as significant.

The *prime contractor's* role in risk management is critical. These responsibilities include defining and documenting a risk management plan and process, modifying and updating the plan and process as necessary throughout the program life cycle, identifying and evaluating program risks, establishing and implementing risk handling efforts, and documenting and reporting risk status. The contractor's risk mitigation strategy will be provided in the PRMP. The contractor will report and discuss the status of the mitigation action of the identified risks in the PRMP during monthly Program Management Reviews (PMRs), and/or Technical Interchange Meetings (TIMs).

The *ITWS Risk Evaluation Board* (IREB) will support the PM in: 1) evaluating and prioritizing risks; 2) recommending plans for mitigation of risks within suitable schedules; 3) recommending responsibilities according to the approved mitigation plans; and 4) performing continuous monitoring of technical, cost, and schedule risk elements. The IREB will be chaired by the PM, and may include several Associate Program Managers (APM) from the matrix support team. The IREB *will have no authority* other than that vested by the PM and will convene based on a schedule established by the PM.

2.0 RISK MANAGEMENT PROCESS

The risk management process consists of: risk identification, assessment, mitigation, control, and monitoring[1].

2.1 Risk Identification

The process begins with the identification of program risk elements. Those already identified as being pertinent to the ITWS include: operational effectiveness, technical performance, schedule, cost, and supportability. The ITWS ORD (Ref. 1.3.1b) has identified specific risk elements in terms of the critical operating issues (COIs) which may impact the potential effectiveness or suitability of ITWS.

Operational effectiveness risk is the probability that the ITWS will not satisfy user needs or provide anticipated benefits. This is a risk element which can be inherent in weather programs when it is difficult to fully anticipate effectiveness due to the wide variety of possible weather environments and operational response scenarios. For example, the ITWS will not be tested in some climatic regimes, and therefore may be subjected to unanticipated regional or local atmospheric conditions. Another related risk is that potential capacity benefits may not be fully realized unless there are changes in operational procedures to use these new ITWS products. The ITWS Operational Test and Evaluation (OT&E) Program is an important element responsible for supporting operational effectiveness validation.

Technical risk is the probability that the developed or produced ITWS will not meet specified requirements. The successful mitigation of risks associated with the design of the software and the coding and integration of the ITWS algorithms by the prime contractor will be a key risk element to be addressed.

Schedule risk is the likelihood of not meeting a specific milestone. Cost risk is the probability that the program will exceed the planned budget. Cost and schedule risks are often outgrowths of technical and programmatic factors. However, they can be independent risks when estimates or goals are unreasonably low, unrealistic, or unattainable. Program cost baselines may be unrealistically low due to: inadequate system descriptions, insufficient historical cost and schedule databases, the lack of sound methods for relating past history to a new program, and/or incomplete estimates (inadvertently omitted items/events, lack of adequate margins,etc).

[1] The process outlined in this plan may be modified and tailored by the ITWS Program Manager -as logically dictated by such factors as program milestones, resource constraints, priorities, or level of risk in the program.

Supportability risk is the likelihood that the system will not be fielded with an adequate logistics support infrastructure. This could be due to a poorly implemented integrated logistics support strategy or inadequately specified maintenance requirements.

Any source of information which allows recognition of a potential problem can be used for risk identification. The PM will establish a process which fosters free-flowing ideas from various sources, and which ensures that any perception of risk from any quarter be considered. Risk processes should be established for each of the major risk elements, including the definition of needed tool sets. For the ITWS program, there is a body of documentation, listed in Section 1.4, which provides information on requirements, testing, science, logistics, and acquisition strategy. The originator and all personnel dealing with this risk element should consult these documents to ensure an adequate understanding of the ITWS environment and program direction. The ITWS Program Work Breakdown Structure (WBS), and Contractor WBS provide an excellent basis for risk identification, as a framework for the technical and programmatic evolution of the program, thus allowing for a determination of the completeness of the program.

A menu of potential specific risk elements is shown in Table 2.1-1. These items are generic in their applicability and may or may not pertain currently to the ITWS, but the risk environment is dynamic, and some of these may be pertinent at a later date.

Risk Recording

Each identified risk will be documented and tracked using the Risk Assessment Form, depicted in Figure 2.1-1, and described in Table 2.1-2. Originators should attempt to perform an initial assessment of the risk, as described in Section 2.2 of this Plan. Upon completion of applicable sections of the Risk Assessment Form, the originator will present the identified risk to the PM (or the PM's designated Risk Coordinator). The PM may then elect to submit the risk element to the IREB for further evaluation, approval and prioritization. The PM may establish a risk data base consisting of these Risk Assessment Forms using automated tools as appropriate. The data base should be structured to allow the PM access to information on individual risks to aid in risk assessment and prioritization.

2.2 Risk Assessment and Analysis

Once a potential risk has been identified, documented and reported to management, the PM will, if appropriate, assign a task to assist in risk assessment or perform a more vigorous risk analysis. The analysis will determine the cause, effects, and magnitude of the risk perceived, and help develop and examine alternative options leading to a mitigation strategy. Risk analysis for elements such as cost, schedule or software development may involve extensive use of tools and statistical techniques.

The assessment of each risk is based on two critical factors: the probability of occurence $P_{(f)}$ and the consequence of occurence $C_{(f)}$. Each risk is rated high, moderate, or low with respect to both $P_{(f)}$ and $C_{(f)}$. The overall risk level, $R_{(f)}$ is derived from these and is also assigned a high, moderate, or low rating.

TECHNICAL/PERFORMANCE RISK ELEMENTS		
- State-of-the-Art Technology: Performance Requirements Packaging Requirements Environmental Requirements Complexity Part Reliability - Technical Sources: Physical Property Material Property Radiation Property - Material Availability: Quantity Quality Alternate vendor Subcontractor/vendor stability - Testing/Modeling: Test facilities Modeling techniques	- Integration/Interface: Adaptability Compatibility Controllability Deployability Design Tolerance Interoperability Quality Control Specifications Standards Survivability Transportability Vulnerability - Program Personnel: Skill levels Availability Travel Requirements	- Software Design: Code estimates Language version Functional Requirements Configuration control Test procedures Critical modules Hardware constraints - Safety: Testing hazard Operation hazard - Failure Modes: Reliability Maintainability Redundancy Fault detection Fault correction Recovery - Energy/Environmental: Energy use Environmental impact
SCHEDULE RISK ELEMENTS		
- Sensitivity to technical - Sensitivity to cost - Dependence on Prior or concurrent result - Turn around time	- Availability of materials - Availability of personnel - Availability of test facilities - Availability of production facilities	- Communication delays/errors - Uncontrollable events: Strikes, Weather, etc - Change in requirements - Test failures
COST RISK ELEMENTS		
- Sensitivity of technical - Sensitivity of supportability - Sensitivity to schedule - Macro-Economic conditions inflation, decreased demand,etc	- Political/Social climate e.g. funding changes - Regulatory changes e.g. new laws, regulations	- Uncontrollable Events: Weather, etc. Strikes - Overhead rates - G&A rates

SUPPORTABILITY RISK ELEMENTS		
- Manpower (customer/user): Numbers, Grades, Specialties, Skill Levels Training - Facilities: Maintenance Simulation	- R&M - Transportability - System safety - Quality Control: Production capability Spares Lead times	- Data management: Formats, Access, Maintenance - Transfer of responsibilities - Interoperability between services/allies - Alternate sources - Configuration Management

Table 2.1-1 Risk Identification Elements Checklist

Risk Item: (a)	Risk No. (b)	Element ©	Origin Date:(d)	Rev. No, Date: (e)	Actionee (f)	Status (g)
Risk Description: (h)						
RISK ASSESSMENT SUMMARY (i)						
Risk Element Assessment				Risk Level (H,M,L)		
Technical:						
Cost/Schedule:						
Supportability:						
Other:						
Recommended Mitigation Plan/Strategy/closure criteria: (j)						
CONCURRENCE/APPROVAL BLOCK (i)						
Originator/Ext/Date:				Evaluation Board Concurrence (initial/Date)		
Analysis Performed by:				Originator's Mgr./Ext/Date:		
Risk Mitigation Actionee/Mgr:						

Figure 2.1-2 Risk Assessment Form

Item	Title	Description	Responsible Party
(a)	Risk Item	Identified risk name	Originator
(b)	Risk Number	Number will be assigned by Coordinator. The number will be sequential according to risk log dates. (e.g. ITWS-001).	Coordinator
©	Risk Element	The general risk element such as operational effectiveness, technical performance, schedule, cost, and supportability.	Originator
(d)	Origination Date	Origination date	Originator
(e)	Revision No/date	Revision number and date	Coordinator
(f)	Actionee	Organization with primary responsibiity for analysis, mitigation planning or other action	Actionee
(g)	Status	I-Initial, A=Assessment, An=Analysis, Mp=Mitigation Planning, W=Working, C=Completed	Coordinator
(h)	Risk Description	A brief description of the identified risk. Description must include a statement on the impact to the program if the risk is not mitigated.	Originator
(i)	Risk Assessment Summary	A brief statement of the risk. Include the probability of failure, consequence of failure, and the risk level (high, moderate, or low)	Originator/ Analyst
(j)	Mitigation Strategy/Plan	A brief description of the analysis results or a plan if risk is to be mitigated (mitigation for moderate or high risks only). Closure criteria/metrics are included.	Analyst
(k)	Concurrence/Approval Block	Include the name, phone number and date of the risk originator, originator's manager, and a person who performs risk analysis.	Program Manager

Table 2.1-2 Risk Assessment Form Instructions

2.2.1 Probability and Consequence of Occurence ($P_{(f)}$, $C_{(f)}$)

The probability of occurence $P_{(f)}$ is the risk that a risk could occur for any element of the program. It frequently involves evaluating aspects of maturity, complexity, or dependency. Figure 2.2.1-1 provides guidance in assigning $P_{(f)}$ to various risks.

The consequence of occurence $C_{(f)}$ is the impact on the program objectives associated with the risk. The consequence of occurence should relate directly to the principle risk elements currently identified. Each risk element is considered in terms of overall importance to the success of the program. Thus the risk elements could be derived by considering the weighted sum of:

$C_{(f)}O$: consequence of occurence operational effectiveness

$C_{(f)}T$: consequence of occurence in program performance/technical;

$C_{(f)}C$: consequence of occurence in program cost;

$C_{(f)}S$: consequence of occurence in program schedule;

where each consequence is assigned a risk if low, medium or high. The value assigned to these factors is derived initially by applying expert judgement. Figure 2.2.1-2 provides guidance in assigning $C_{(f)}$ to various risks.

Rating	Characteristics
High (3)	High likelihood to certainty of risk event occurrence (70 to 100% probability) Factors: -Knowledge, experience base very limited or lacking -Many schedule interdependencies, high dependency on new FAA systems or systems not fielded -Cost unknown: inadequate basis for estimate -Technology: Maturity-state-of-the-art-not beyond experimental or analytical stage; Complexity-high; Dependency-high -No plans (prototyping, margins, etc) to minimize unknown -Very tight/impossible schedule: highly success oriented
Medium (2)	Good Possibility of Risk Event Occurrence (30 to<70% probability) Factors: -Knowledge or experience in some elements -Some schedule interdependencies mainly to existing or near-term FAA systems -Plans to minimize unknowns generally complete, some uncertainties -Cost Factors not certain -Technology: Technology maturity- available, prototype may have been tested in relevant environment -Tight schedule
Low (1)	Slight to moderate possibility of risk event occurrence (<30% probability) Factors: -High knowledge & experience base in subject environment -Complete, achievable plans to minimize unknowns -Adequate schedule margin -Few or no schedule interdependencies -Cost factors understood -Technology: within state of the art, off-the-shelf, prototype tested

Figure 2.2.1-1 Rating Probability of Occurence $P_{(f)}$

Rating	Operational Factor $C_{(O)}$	Technical Factor $C_{(t)}$	Cost Factor $C_{©}$	Schedule Factor $C_{(s)}$
(Low)	Confidence that the ITWS products will result in improved capacity, etc	Small reduction in technical performance	Cost estimates exceed budget by <5 percent	Minor slip in schedule (less than 1 month), some adjustment in milestones required
(Mod)	Some doubt that the ITWS products will result in improved capacity, etc	Some reduction in technical performance	Cost estimates increased by 5 to 30 percent	Small slip in schedule
(High)	Significant concern that the ITWS products will result in improved capacity, etc	Technical performance cannot be achieved	Cost estimates increased in excess of 30 percent	Large schedule slip that affects segment milestones or has possible effects on program milestones

Figure 2.2.1-2 Rating Consequence of Failure $C_{(f)}$

2.2.2 Risk Level/Factor (R_f)

The *overall* risk level, $R_{(f)}$, is a function of both the probability of failure $P_{(f)}$ and the consequence of failure $C_{(f)}$. The risk mitigation strategy will be implemented and prioritized using this parameter. Figure 2.2.2-1 provides guidance as to how to assess the overall level of risk given ($P_{(f)}$,$C_{(f)}$), and when mitigation strategies are warranted. For example if either $P_{(f)}$ or $C_{(f)}$ is low, or one is low while the other is medium probability, the overall risk is considered low. If the probability for both is medium or one is high and the other low, the risk is considered medium. If one parameter is high and the other at least medium, the risk is high. The need for mitigation is based on the magnitude of the risk factor. If the overall risk $R_{(f)}$ is high, risk mitigation is required; if $R_{(f)}$ is medium, it is desirable. No special risk mitigation is required if $R_{(f)}$ is low, although risk monitoring may be warranted.

$C_{(f)}$	Risk $R_{(f)}$*		
High	Med	High	High
Med	Low	Med	High
Low	Low	Low	Med
$P_{(f)}$	Low	Med	High
*Shading indicates mitigation required or desired			

Figure 2.2.2-1 Rating Overall Risk Level $R_{(f)}$

2.2.3 Risk Analysis Tools

Many FAA programs have utilized automated tools which can be used in the risk analysis process. These include schedule network analysis tools such PERT, and ARTEMIS. In addition various cost risk/WBS simulation tools have been used such as SASET, @RISK and others. The PM will establish a menu of tools which allow Government tracking of risk elements prior to ITWS contract award. The selection and cost of these tools will depend on the overall level of risk in the risk elements at that time.

2.3 Risk Mitigation

The most critical factor in determining a risk mitigation strategy is the risk level. The selection of mitigation strategy is based on trade-offs between relevant factors and supporting data, such as risk level, available alternatives, cost, trends, historical information, and environments. The following strategies are used in risk mitigation:

a) Avoidance is a drastic approach which could involve scope changes such as modification, relaxation or elimination of requirements. This approach is usually applied to only the high $P_{(f)}$ risk levels.

b) Transfer is an approach whereby risk is transferred among components (e.g. reallocation from hardware to software), subsystems, subcontractors, etc., to obtain the most successful overall program strategy.

c) Control is the most common of all risk handling techniques. Control is the process of continually monitoring and correcting the condition. Control involves many different strategies such as special testing, detailed personnel training, special procedures, margin allocation, development of a second source, etc.

Once a risk item is properly identified and analyzed, an alternative analysis will be conducted, and the mitigation strategy determined. If the strategy is other than "avoidance", a mitigation plan will be prepared and tracked. The format and complexity of the mitigation plan will be determined by the PM. When dealing with the prime contractor, the content and format of the mitigation plan should be placed under contract. The plan will a) identify and list possible alternatives/corrective actions; b) describe fallback options and financial contingencies; c) arrange the list in hierarchical order, from best alternative at the top to least effective action at the bottom, and d) list the "best choice" and enumerate the remaining alternatives. The prime contractor will report status of all risk item mitigation plans at PMRs or other intervals as contractually agreed.

2.4 Risk Evaluation Control

Once a Risk Mitigation Plan has been developed, it will be forwarded to the IREB. The IREB will recommend a schedule and assign responsibility to the appropriate organization for implementation. Depending on the tasks involved, the assignment of risk management responsibilities may involve the FAA, prime contractors, or a joint effort. Should the recommended mitigation plan be unacceptable by the IREB, the identified risk will be reassessed and a revised plan will be developed and forwarded to the Board for reevaluation. The ITWS Program Office will notify the contractor of all identified risk items that are applicable to the contractor for mitigation. The contractor will then report the status of the risk reduction activities during each PMR or as required.

2.5 Risk Monitoring

Once a risk mitigation plan has been established, accurate documentation and continued evaluation are important to ensure that 1) the expected results are obtained, 2) factors attendant to the risk have not changed, and 3) no new risks have been introduced. Risk assessment and mitigation strategies will be documented and monitored using the Risk Assessment Form and risk assessment data base, and distributed as required. This database in conjunction with the ITWS Matrix Team meetings, the monthly PMRs, and various program status reports will be used to track risk management activities.

3.0 RISK REDUCTION

3.1 ITWS Management Strategies for Risk Reduction

As stated in Sec 2.1, the key risk elements include operational effectiveness, cost, schedule, technical and supportability. This Plan has established a process for dealing with these risks. General management strategies for monitoring and controlling the major risk elements are listed in Table 3.1.

Risk Element	**Management Strategy**
Cost	- Identify key WBS cost sensitivities-especially for the elements of software, interfaces, documentation and logistics; - Conduct periodic cost risk analyses using cost risk tools;
Schedule	- Evaluate WBS for schedule risk drivers, develop and evaluate schedules with varying confidence levels, identify critical paths; identify all inter-dependencies; - Implement schedule risk evaluation tools; - Conduct periodic review meetings with contractor over WBS schedule, inter-dependencies, emphasize risk reduction along critical path.
Technical	- Ensure GFE documentation and algorithms adequate for implementation by prime contractor; - Use verification and validation contractor to evaluate prime contractor DT&E; - Implement contractor RMP to continually evaluate hardware, software risks - Software risk-implement comprehensive risk reduction strategy as appropriate and as funding allow: - Contractor-supplied reporting of management and technical software metrics which indicate progress toward established objectives (e.g. resource utilization curves, etc); - Use of algorithm provider for analysis of contractor software design and coding, when called upon - Adherence to software development documentation and review standards
Operational Effectiveness	- Ensure full evaluation of ITWS demonstration validation testing results, with ATC feedback; - Ensure full analysis of benefits; - Conduct FAA OT&E emphasis on Critical Operational Issues
Supportability	- Conduct RMA analysis and testing, development and implementation of ITWS ILSP

Table 3.1-1 Key Risk Elements and Management Strategies

3.2 ITWS Testing and Evaluation Program

The approach to testing and evaluation is contained in the ITWS Test and Evaluation Master Plan (TEMP). It requires the development of an FAA development test and evaluation (DT&E) program and includes a proviso for a contractor DT&E plan. It establishes objectives for the FAA's Operational Test and Evaluation Plan (OT&E). An important aspect of the test and evaluation program is identification of critical operating issues (COIs) which focus the test program on significant technical and operational risks.

Product maturity has been a cornerstone of the ITWS test and evaluation program. Demonstration and validation tests have been conducted during the 1993 summer operations at Orlando and Dallas/Fort Worth, and the 1994 tests conducted at Memphis and Orlando. During these tests all ITWS IOC products (e.g. storm motion and extrapolation, terminal winds, anomalous propagation editing) were evaluated in actual airport environments. Questionnaires were distributed to users at the end of the tests and were analyzed by ACW-200D, and documented in Refs 1.3.3a, and 1.3.3b. *[[To be provided: results of the 1994 tests at Memphis.*]]. These constitute the most significant aspects of determine product maturity, since the prime contractor will be coding the algorithms which were used in these tests.

The ITWS program is dependent upon our scientific understanding of: 1)the weather phenomena impacting the terminal ; 2) methods for measuring these phenomena; and 3) assimilation techniques leading to processing of these measurements. To ensure that the science was mature enough, ARD-80 sponsored an independent science panel to evaluate the ITWS products. The Science Panel's findings were positive, indicating minimal risk in the scientific aspects of the program.

Beyond the demonstration and validation tests, Ref (1.2.3b) describes the OT&E program to be conducted by ACW-200D in technical and operational areas.

LIST OF ACRONYMS

APM	Associate Program Manager
COI	Critical Operational Issue
DID	Data Item Description
DT&E	Development Test and Evaluation
FAA	Federal Aviation Administration
GFE	Government Furnished Equipment
IOC	Initial Operating Capability
IREB	ITWS Risk Evaluation Board
ITWS	Integrated Terminal Weather System
ORD	Operational Requirements Document
OT&E	Operational Test and Evaluation
PM	Program Manager
PMR	Program Management Review
PRMP	Contractor Program Risk Management Plan
RMP	Risk Management Plan
TEMP	Test and Evaluation Master Plan
TIM	Technical Interchange Meeting
WBS	Work Breakdown Structure